DHCP and Router Advertisement Options for Encrypted DNS Discovery

https://tools.ietf.org/html/draft-ietf-add-dnr

March 2021

M. Boucadair (Orange)
T. Reddy (McAfee)
D. Wing (Citrix)
N. Cook (Open-Xchange)
Tommy Jensen (Microsoft)

Active Issues

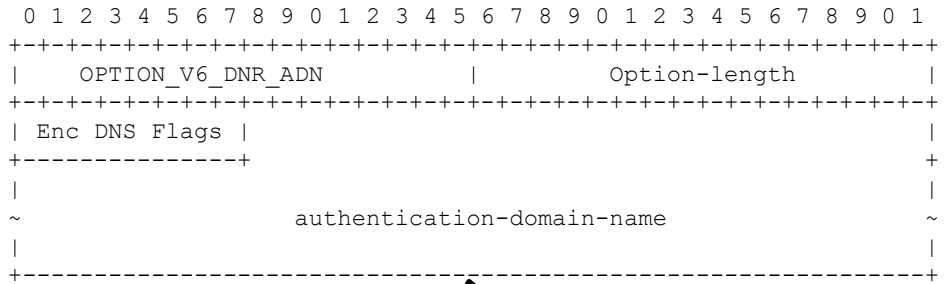
- https://github.com/ietf-wg-add/draft-ietf-add-dnr/issues (3 open)
  - Source xml, but will prepare a source md file soon

- Will focus on this issue:

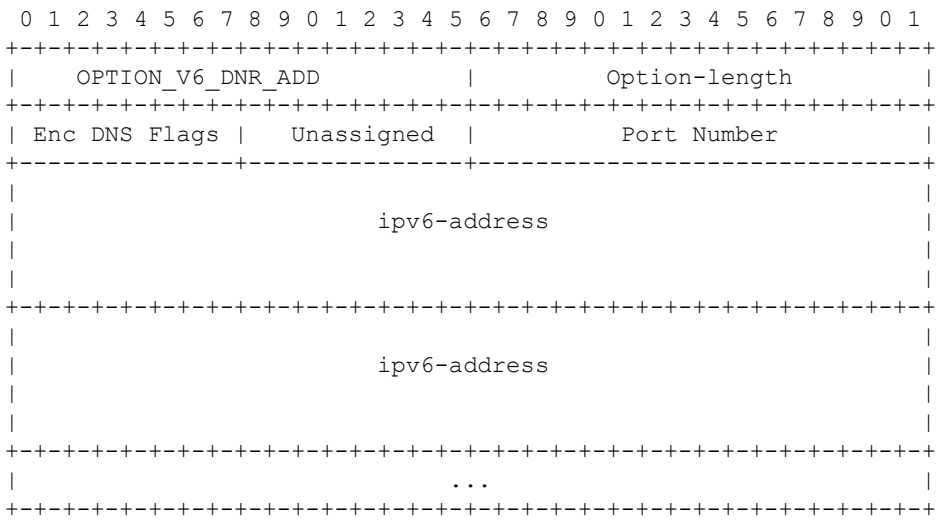
*"Most of the draft seems to concern the **exact formats of how to deliver resolver information** over DHCP/RA, and I think these formats **should largely be rewritten to harmonize with DEER**." (Ben Schwarz)*

Which Information is Discovered?

- Return the ***minimal information*** to establish an authenticated connection with a DNS resolver
- Two options are defined



Follow the guidelines in RFC7272



Relationship with DDR

"Upon discovery of a DoH resolver (Sections 4, 5, and 6), ***the DoH client may contact that DoH resolver to retrieve the list of supported DoH services using DDR [I-D.ietf-add-ddr]****. This will allow the client to discover the* ***resolver's supported DoH templates or DoH resolvers that the discovered resolver designates using DNS SVCB queries*** *[I-D.schwartz-svcb-dns]. The designated DoH resolvers and DoH resolver discovered using DHCP/RA may be hosted on the same or distinct IP addresses." (Excerpt from draft-ietf-add-dnr)*

Why Defining Two Options?

- The initial design in 05/20 proposed ***the ADN option only*** while the address is conveyed in the legacy Do53 @ List

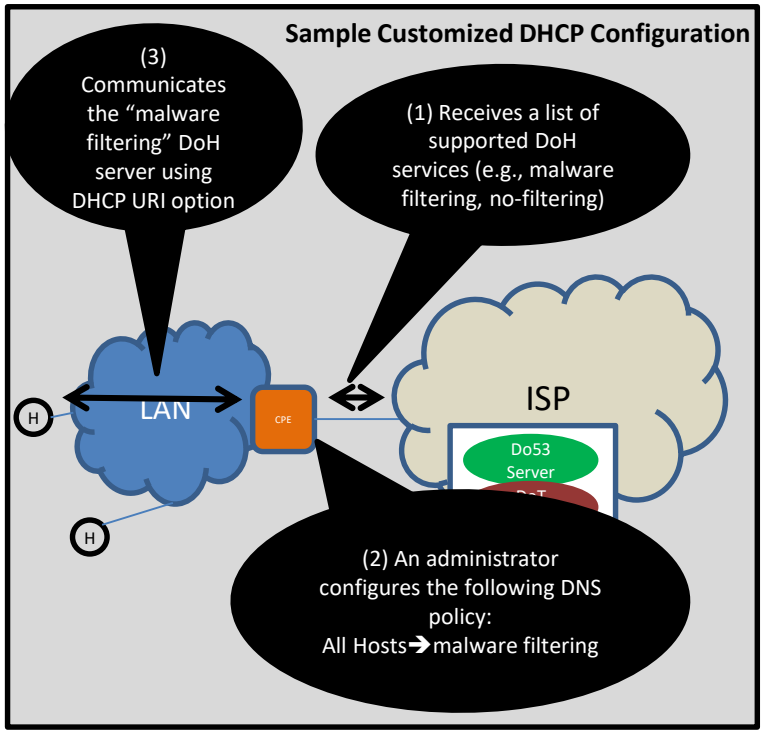
- That design was abandoned because it was suboptimal:
  - It requires ***probing*** if the designated encrypted DNS services are not available on the same IP address(es)
  - It requires ***falling back to Do53*** to discover the IP addresses and the alternate port number

Issue: DNR Options Should be Isomorphic to DDR Information

- What additional information do we need to convey in the options?
  - URI Templates?
  - Other information?

Issue: URI Templates in RA/DHCP?

- Why?
  - Provide a customized DNS configuration within a local network
- There are trade-offs
  - Some issues
    - May ***increase the size*** of RA/DHCP messages
  - Some advantages
    - Clients can ***immediately use*** the service(s); no need for extra queries to retrieve the URIs
    - Does ***not interfere*** with DNS exchanges to "customize" the available services
    - SVCB DNS does not mandate DNSSEC and the Do53 response can be modified by an attacker
    - RA/DHCP is not subject to ***external attacks***



Suggestions:

- Define RA/DHCP options to convey URI Templates
- These options, when available, take precedence over DDR

Issue: No @List is Returned

- If the client receives a Do53 @List and an ADN, should the client use that list to resolve the ADN or should that list be assumed as locators to reach encrypted DNS servers?

Suggestion:
- Recommend to always return a list of encrypted DNS @es, unless Do53 and encrypted DNS terminate on the same @es

Motivation:
- Optimize the message size

Next Steps

- Implement the outcome of the discussion
- Edits and clarification to take into account Michael and Yan's comments
  - https://github.com/ietf-wg-add/draft-ietf-add-dnr/issues/
- Please review and share comments

Backup

DNR Design Assumptions

- ***One or more encrypted DNS servers*** can be advertised by a network, e.g., DoT+DoQ+DoH
- The ***same or distinct*** Authentication Domain Names may be used for DoT, DoH, DoQ, etc.
- Available encrypted DNS servers may run on the ***same or distinct IP addresses***
- An encrypted DNS service (e.g., DoT, DoQ) may use a ***non default port number***

Typical Communication Flow

- Clients ask for one or more encrypted DNS (e.g., DoT, DoH) by ***setting dedicated flags*** in the options
  - A client that is interested in any encrypted DNS will set all the flags
- Servers reply with ADN(s), a list of IP addresses, and a port number, if the requested encrypted DNS is supported
  - It is ***RECOMMENDED to return both an ADN + a list of IP addresses***
  - ***One or more*** encrypted DNS types may be returned
  - These services may be bound to the ***same or distinct IP addresses***
  - ***Alternate port numbers*** can be returned when default port number are not in use
  - If a list of IP addresses is returned, that list is ***ordered***
  - Some recommendations to ***optimize*** the message size are included

Sync DDR and DNR

- DHCP servers can issue SVCB queries and cache the results

- See, for example, **RFC 7969**

" Depending on the server capability and configuration, it may cache resolved responses for a specific period of time, repeat queries every time, or even keep the response until reconfiguration or shutdown. For more detailed discussion, see Section 7 of [RFC7227].”